In accordance with the invention, the dispatch authentication involves an authenticator that operates as a non-interested third party with respect to the sender and the recipient. The dispatch is transmitted through a dispatcher between the sender and the recipient. As part of the dispatching process, the authenticator associates the contents of the dispatch with dispatch-related information (e.g., the how, when and whom of the dispatch) by generating a representation of at least the contents, time, and destination of the dispatch. This representation, which is used as the authentication information, is then secured by the authenticator to prevent tampering, such as by the sender or the recipient. The autencitaion information enables the sender to demonstrate the authenticity of the dispatch and its contents.

Turning now to the Office Action, the Office Action rejected claim 75 under 35 U.S.C. § 112, second paragraph. The Office Action considered the term "at least part of" in claim 75 as being indefinite. Applicants have amended claim 75 to recite that the apparatus is combined in whole or in part with the dispatcher. This claim language is intended to clarify that the authenticator may be combined in whole or in part with the dispatcher, i.e., some or all of the tasks of the authenticator may be performed by the dispatcher.

The Office Action rejected claims 64-66, 69, 71-79, 92-96, 98, 100, 101, 103-110, 123-127, 131, 132, 134, 137-140, 144, 145, 149-151, 153, 154, and 160 under 35 U.S.C. § 102(b,e) as being anticipated by Bouricius et al. U.S. Patent 4,326,098. The

Office Action asserted that Bouricius et al. disclose a system based on the concept of a vault or central authority, and equated the vault with the dispatcher recited in the claims. The Office Action also rejected claim 159 under 35 U.S.C. § 102(b) as being anticipated by Schneier, Applied Cryptography, 1st edition. The Office Action further rejected claims 68, 80, 97, 111, 133, 147, 15, 158, and 161 under 35 U.S.C. § 103(a) as being unpatentable over Bouricius et al. Nevertheless, the Office Action indicated that claims 67, 70, 81-91, 99, 102, 112-122, 128-130, 135, 136, 141-143, 146, 148, 152, 156, and 157 would be allowable if rewritten in independent form.

Because the Bouricius et al. patent is the main reference relied upon in the Office Action to support the rejections, applicants discuss here the teachings of this reference and point out the fundamental differences between this reference and the invention. Bouricius et al. disclose an authentication process performed between a sender A and a recipient B, wherein both the sender and the recipient play an active role, that is, they both actively participate and cooperate in the evidence generation process. The process according to Bouricius et al. is an electronic equivalent of the familiar paper document signing, where both parties A and B sign the same document, and where each party ends up having the document D signed by the other party, together with the signing time. The process of Bouricius et al. involves a vault, which acts as a trustee assisting the parties in authenticating the identity of each other, in verifying the

time of the exchange, and in establishing a safe or secure communication. The vault however, does not play any active role in the generation of the evidence, nor in the generated evidence itself, i.e., one cannot later verify from the evidence blocks C1 or C2 that they have been witnessed by the vault.

This process of Bouricius et al. and the present invention have totally different approaches that are premised on opposite presumptions. Specifically, Bouricius et al. rely on the cooperation between the sender and the recipient, and assume a mutually cooperative environment. Under the approach of Bouricius et al., to obtain evidence of a transmission C2, the sender A is totally dependent on the recipient B's willingness to cooperate (i.e., to sign the received document D and return it to A).

In sharp contrast, the present invention assumes that such cooperation is not or might not be reachable,such as in the cases where a dispute between the parties arises or where the parties are members of different and disjoint networks. The process according to the present invention overcomes this problem by employing an independent, non-interested authenticator not associated with either the sender or the recipient to generate the evidence of the dispatch and secure the evidence, thereby playing an active and crucial role in the evidence generation process. In this process, the sender does not rely on the receiver's cooperation. In fact, the recipient does not play any active role in generating the authentication-information for

evidencing the dispatch. Thus, the present invention is very different in scope, goals and technique from the process of Bouricius et al.

In this regard, applicants believe that the original claims were already clear in that the recipient is not the one generating and securing the authentication information, in contrast to the role of the recipient in the process of Bouricius et al. Nevertheless, to further emphasize this important distinction between the present invention and the process of Bouricius et al., the claims are amended to specify that the generating and securing of the authentication information are performed by an authenticator functioning as a non-interested third party with respect to the sender and the recipient. Support for this claim limitation is found, for example, on pages 7-8 of the specification, where it is stated that:

> *The present invention also encompasses all types of methods and apparatuses which provide and/or associate the dispatch information with the contents in a relatively secure or reliable manner. The terms "relatively secure" and "reliable" herein mean "reasonably tamper-proof" or "tamper-detectable", i.e., that it is assured that the authentic information elements are provided and associated in a reliable manner, for example by a non-interested third party or by a device or by a combination of both, and furthermore, that the associated authentication-information is secured against fraudulent actions such as disassociation, modification, replacement etc., attempted by an interested party such as the sending or receiving party, at least to the extent that such actions are detectable.*

Further support can be found in dependent claims 93, 124, 136, 148 and 157 , where it is emphasized that the authenticator is not associated with either the sender or the recipient.

Applicants have amended all independent claims to include this limitation. Thus, all the pending claims as amended are clearly distinguishable from the teachings of Bouricius et al.

In making the Section 102 rejection of claim 64, the Office Action considered the vault of Bouricius et al. to be the dispatcher of the claimed invention. (Applicants believe that the Office Action actually meant the "authenticator", since it is the authenticator that is responsible for generating and securing the dispatch authentication information.) The vault of Bouricius et al., however, does not play any active role in the generation or securing of the evidence and is therefore not the authenticator of the claimed invention. The role of the vault in the process according to Bouricius et al. is to act as a trustee assisting the parties in authenticating the identity of each other, in verifying the time of the exchange and in establishing safe or secured communications. This is an important distinction of the claimed invention from Bouricius et al., wherein the vault, in contrast to the present invention, does not secure the evidence against tampering by the parties, but rather utilizes encryption solely for the purpose of establishing safe and secure communications with either of the parties A and B.

Specifically, the vault utilizes A's key K_A to communicate with A. Since A knows his key, encrypted data blocks sent by the vault become readily insecure as they reach A. The same applies to communications between the vault and B. The only real valuable evidence that A holds is C2, consisting of B's digital

signature on the original message D and the time it has been signed. Similarly, B holds C1, consisting of A's digital signature on the original message D and the time it has been signed. The vault merely assists in inspecting the process to ensure that the parties are those from whom the communications originated. The vault, however, does not generate and/or secure the evidence regarding the dispatch.

Moreover, according to the teachings of Bouricius et al., there is no need for the vault to secure the evidence blocks C1 and C2. This is because those blocks are already secured. Specifically, C1 is held by B and is secured from tampering by B because it is encrypted (signed) with A's secret key K_A, and similarly C2 is held by A and is secured from tampering by A because it is encrypted (signed) with B's secret key K_B.

In view of the above discussion, it is clear that due to the fundamental differences in the approaches of the present invention and Bouricius et al., Bouricius et al. could not have anticipated the claimed invention. To recapitulate, Bouricius et al. do not teach or suggest the use of an authenticator that is not associated with either the sender or the recipient to create and secure authentication information for the dispatch. Accordingly, it is believed that all the claims rejected under Section 102 are (in their amended form) not anticipated by Bouricius et al. and should therefore be allowable.

Moreover, the Bouricius et al. patent was the only reference cited in the Office Action for supporting the Section 103

rejection. As discussed above, the Bouricius et al. process relies upon the mutual cooperation of the sender and recipient of the dispatch, and is based on the premise that the recipient will and can cooperate in the process. Since this premise is opposite to that of the present invention, Bouricius et al. provide no suggestion or motivation for the use of an independent third party, namely the authenticator, to create and secure the authentication information. In fact, due to its emphasis on the cooperation and active involvement of the recipient, Bouricius et al. may even be said to teach away from the invention, which does not require the recipient to play any part in the generation of the dispatch authentication information. Accordingly, Bouricius et al. could not have rendered the claimed invention obvious, and the claims rejected in the Office Action under Section 103(a) should be allowable as amended.

Although it is believed that the above discussion has established the allowability of the claimed invention over Bouricius et al., applicants nevertheless address here some other assertions in the Office Action regarding the teachings of Bouricius et al. for the purpose of facilitating any further review of this reference. The Office Action stated:

> ...Bouricius et al. disclose encrypting and step-coding the information to resist or indicate tampering by either the sender or receiver. (col. 9: 31-46)
>
> ...Bouricius et al. disclose associating and securing the dispatch-related information with the contents by generating authentication-information. (col. 9:24-26 and 31-46, where the authentication-information is the original ciphertext

from the sender to be later used for arbitration if a dispute arises)

If the Office Action was referring to the encipherment performed by the vault, then the information is not tamper-proof, since the vault enciphers the information sent to B using B's key K_B, which B can readily decipher (using Bouricius et al. Fig.1-2 Block Σ^{-1}). The same applies to information sent by the vault to A. If, on the other hand, the Office Action was referring to the encipherment by the sender and the recipient, it is crucial to point out that C1 has been generated by A (similar to A's signature on paper documents), and that C2 has been generated by B (similar to B's signature on paper documents). In both cases, C1 and C2 have been generated by the parties A and B themselves, and not by anybody else, in particular not by the vault. Therefore, in light of the claim amendment, the rejections are no longer applicable.

Claim 159 was the only claim that the Office Action rejected based on a reference other than Bouricius et al. Specifically, the Office Action rejected claim 159 as being anticipated by Schneier, which explains a public-key certificate. Schneier, however, does not anticipate or suggest the claimed invention of claim 159. The public-key certificate described by Schneier is nothing more than the Certificate-Authority's signature certifying the public key. The process should be regarded as a sender (in this context the Certificate-Authority) sending information (public key) to a recipient (the user or public key

owner) and certifying the contents and time with the sender's (the Certificate-Authority) digital signature. This is equivalent to the process of any sender sending out a digitally signed message to a recipient. Thus, such a public-key certificate is fundamentally different in nature from the certificate recited in claim 159, as it cannot be used for attesting to the dispatch and the contents of the dispatch. Furthermore, claim 159 as amended includes the limitation that the authentication data are generated by an authenticator that is a non-interested third party to the sender and the recipient. The process of Schneier lacks such an authenticator. In this regard, it is noted that the Certificate-Authority should not be viewed as such an independent third party. This is because the Certificate-Authority is actually the "sender" in the process of Schneier and cannot be both a sender and an independent, non-interested, third party at the same time.

Alternatively, the process can be considered equivalent to that described by Bouricius et al., where the sender A (the user) sends data D (public key) to a recipient B (the Certificate-Authority). B signs the data D along with time BC and A's name, thereby producing C2 (the Certificate) of Bouricius et al. This process not only lacks a third party but also, as already thoroughly discussed above, is different than the claimed invention due to the need for the recipient's participation. Accordingly, claim 159 as amended is not anticipated or suggested by Schneier and should be allowable.

Conclusion

Applicants submit that the application is now in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue.

If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

Y. Kurt Chang - Reg. No. 41,397
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: February 3, 2000